

02.02.01

JP 01/772 日本国特許庁  
EU PATENT OFFICE  
JAPANESE GOVERNMENT

774

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application:

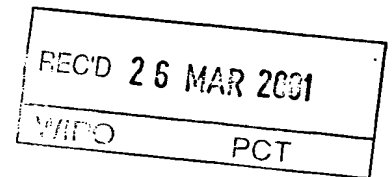
2000年 8月 2日

出願番号  
Application Number:

特願2000-234741

出願人  
Applicant(s):

ソニー株式会社



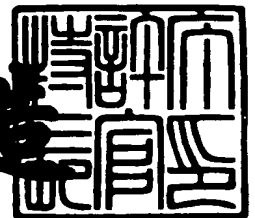
09/937797

PRIORITY  
DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2001年 3月 2日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2001-3015164

【書類名】 特許願

【整理番号】 0000171303

【提出日】 平成12年 8月 2日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明者】

    【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

    【氏名】 金巻 裕史

【発明者】

    【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

    【氏名】 佐竹 清

【特許出願人】

    【識別番号】 000002185

    【氏名又は名称】 ソニー株式会社

    【代表者】 出井 伸之

【代理人】

    【識別番号】 100094053

    【弁理士】

    【氏名又は名称】 佐藤 隆久

【手数料の表示】

    【予納台帳番号】 014890

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9707389

【プルーフの要否】

要

【書類名】 明細書

【発明の名称】 通信制御装置、通信システムおよびその方法

【特許請求の範囲】

【請求項 1】

単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を制御する通信制御装置であって、  
前記第 1 の通信装置を識別するための装置識別情報を記憶する記憶手段と、  
前記第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報を含む要求を前記第 2 の通信装置に送信する送信手段と、  
前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する受信手段と、  
前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する制御手段と  
を有する通信制御装置。

【請求項 2】

前記制御手段は、  
前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記第 2 の通信装置に所定の通知を行う  
請求項 1 に記載の通信制御装置。

【請求項 3】

前記制御手段は、  
前記応答に含まれる装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う  
請求項 1 に記載の通信制御装置。

【請求項 4】

前記送信手段は、

前記第 1 の通信装置から受信した利用者識別情報と、当該第 1 の通信装置に対応する前記装置識別情報とを含む前記要求を前記第 2 の通信装置に送信する

請求項 1 に記載の通信制御装置。

【請求項 5】

前記記憶手段は、

前記第 1 の通信装置から受信した前記装置識別情報を記憶する

請求項 1 に記載の通信制御装置。

【請求項 6】

前記記憶手段は、

当該通信制御装置の電源が投入されたときに前記第 1 の通信装置から受信した前記装置識別情報を記憶する

請求項 5 に記載の通信制御装置。

【請求項 7】

前記制御手段は、

前記第 1 の通信装置と前記第 2 の通信装置との間の通信履歴を前記記憶手段に書き込む

請求項 1 に記載の通信制御装置。

【請求項 8】

前記制御手段は、

前記応答に含まれる前記第 2 の通信装置の処理結果を、前記要求の送信元の前記第 1 の通信装置に送信する

請求項 1 に記載の通信制御装置。

【請求項 9】

前記制御手段は、

前記受信手段から受信した情報に応じて、待機状態にある前記第 1 の通信装置が動作状態になるように制御する

請求項 1 に記載の通信制御装置。

【請求項 10】

前記制御手段は、

前記第 1 の通信装置が接続されたネットワークと、前記第 2 の通信装置が接続されたネットワークとの間の通信を制御する

請求項 1 に記載の通信制御装置。

【請求項 1 1】

前記制御手段は、

ゲートウェイとしての処理を行う

請求項 1 0 に記載の通信制御装置。

【請求項 1 2】

前記装置識別情報は、前記第 1 の通信装置の製造元で付された当該通信装置を一意に識別可能な識別子である

請求項 1 に記載の通信制御装置。

【請求項 1 3】

前記利用者識別情報は、登録した利用者に予め割り当てられた識別子である

請求項 4 に記載の通信制御装置。

【請求項 1 4】

前記受信手段は、

前記第 2 の通信装置が行った認証処理の結果を含む前記応答を前記第 2 の通信装置から受信する

請求項 1 に記載の通信制御装置。

【請求項 1 5】

単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信システムであって、

前記通信制御装置は、

前記第 1 の通信装置を識別するための装置識別情報を記憶する第 1 の記憶手段と、

前記第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報と利用者識別情報とを含む要求を前記第 2 の通信装置に送信する第 1 の送信手段と、

前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する第 1 の受信手段と、

前記応答に含まれる前記装置識別情報と前記第 1 の記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記第 1 の記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する制御手段と

を有し、

前記第 2 の通信装置は、

前記要求を受信する第 2 の受信手段と、

前記利用者識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する第 2 の記憶手段と、

前記要求に応じて所定の処理を行う処理手段と、

前記要求に含まれる前記利用者識別情報に対応する前記送信先の情報を前記第 2 の記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果と前記要求に含まれる前記装置識別情報とを対応付けて送信する第 2 の送信手段と

を有する

通信システム。

#### 【請求項 1 6】

単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信方法であって、

前記第 1 の通信装置から前記通信制御装置に出された要求に応じて、当該第 1 の通信装置に対応する装置識別情報と利用者識別情報とを含む要求を前記通信制御装置から前記第 2 の通信装置に送信し、

前記第 2 の通信装置において、受信した前記要求に応じた所定の処理を行い、

前記第 2 の通信装置において、前記要求に含まれる前記利用者識別情報に対応する送信先の情報に基づいて、前記処理の結果と前記要求に含まれる前記装置識別情報とを含む応答を前記通信制御装置に送信し、

前記通信制御装置において、受信した前記応答に含まれる前記装置識別情報と、予め保持した前記第 1 の通信装置の前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、正当な前記第 1 の通信装置によるものであるかを判断する

通信方法。

【請求項 1 7】

前記通信制御装置は、

前記応答に含まれる前記装置識別情報と予め保持した前記第 1 の通信装置の前記装置識別情報とが一致しない場合に、前記第 2 の通信装置に所定の通知を行う  
請求項 1 6 に記載の通信方法。

【請求項 1 8】

前記通信制御装置は、

前記応答に含まれる前記装置識別情報と予め保持した前記第 1 の通信装置の前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う

請求項 1 6 に記載の通信方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、例えば電子商取引情報を認証などの処理を行う際用いられる通信制御装置、通信システムおよびその方法に関する。

【0 0 0 2】

【従来の技術】

インターネットなどのネットワークを介して商品等の販売や代金の決済を行う電子商取引が普及している。

このような電子商取引を用いて利用者が商品等を購入する場合には、例えば、利用者が店舗や各家庭に設置されたパーソナルコンピュータなどの発注者端末装置を操作して、ネットワークを介して、商品等の販売を行うサーバ装置にアクセスを行う。これにより、サーバ装置から発注者端末装置に商品の写真、特性およ



び価格などの情報が提供され、発注者端末装置のディスプレイに表示される。利用者は、このような情報を見ながら、購入を希望する商品等を選択し、選択した商品等の発注処理を行う。発注処理は、利用者個人を特定する個人ID情報、発注する商品等を指定した情報およびその決済方法等の情報を、発注者端末装置を操作して入力し、これをネットワークを介してサーバ装置に送信する。

#### 【0003】

このような電子商取引では、ネットワーク銀行などが、ネットワークを介した取引に関する決済業務を行うが、当該決済を行うに当たって、決済対象となる電子商取引の内容の正当性が認証されている必要がある。

従って、電子商取引では、このような電子商取引の内容の正当性を認証する処理を行う認証装置が用いられる。当該認証装置を用いた認証業務は、ネットワーク銀行、あるいは他の信頼性のある機関が行う。

#### 【0004】

##### 【発明が解決しようとする課題】

ところで、上述したような認証装置では、例えば、個人ID情報を他人が不正に取得した場合に、当該他人は、その個人ID情報を用いて、認証装置に対して認証要求を出すことができ、不正な取引が行われてしまう可能性があるという問題がある。

また、家庭内に複数の端末装置を設けた場合に、外部のネットワークを介して行われる電子商取引やセキュリティに関する機能を端末装置毎に持たせると、効率が悪いと共に、例えば家庭単位で通信履歴を管理するときに不便である。

#### 【0005】

本発明は上述した従来技術の問題点に鑑みてなされ、不正に取得した他人の個人ID情報に基づいて不正な認証手続が行われることを回避する通信制御装置、通信システムおよびその方法を提供することを目的とする。

また、本発明は、複数の端末装置を用いてネットワークを介した電子商取引などを行う場合に、当該電子商取引に必要な機能の割り当て、並びに通信履歴の管理を効率的に行うことができる通信制御装置、通信システムおよびその方法を提供することを目的とする。

## 【 0 0 0 6 】

## 【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第1の発明の通信制御装置は、単数または複数の第1の通信装置からの要求に応じてネットワーク上の第2の通信装置で処理を行うことに関しての通信を制御する通信制御装置であって、前記第1の通信装置を識別するための装置識別情報を記憶する記憶手段と、前記第1の通信装置からの要求に応じて、当該第1の通信装置に対応する前記装置識別情報を含む要求を前記第2の通信装置に送信する送信手段と、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第2の通信装置から受信する受信手段と、前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第1の通信装置によるものであるかを判断する制御手段とを有する。

## 【 0 0 0 7 】

第1の発明の通信制御装置の作用は以下になる。

送信手段、第1の通信装置からの要求に応じて、当該第1の通信装置に対応する前記装置識別情報を含む要求を第2の通信装置に送信する。

そして、受信手段が、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第2の通信装置から受信する。

次に、制御手段によって、前記受信した応答に含まれる前記装置識別情報と記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第1の通信装置によるものであるかを判断する。

## 【 0 0 0 8 】

また、第1の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記第2の通信装置に所定の通知を行う。

## 【 0 0 0 9 】

また、第 1 の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う。

【 0 0 1 0 】

また、第 1 の発明の通信制御装置は、好ましくは、前記送信手段は、前記第 1 の通信装置から受信した利用者識別情報と、当該第 1 の通信装置に対応する前記装置識別情報とを含む前記要求を前記第 2 の通信装置に送信する。

【 0 0 1 1 】

また、第 1 の発明の通信制御装置は、好ましくは、前記記憶手段は、前記第 1 の通信装置から受信した前記装置識別情報を記憶する。

【 0 0 1 2 】

また、第 1 の発明の通信制御装置は、好ましくは、前記記憶手段は、当該通信制御装置の電源が投入されたときに前記第 1 の通信装置から受信した前記装置識別情報を記憶する。

【 0 0 1 3 】

また、第 1 の発明の通信制御装置は、好ましくは、前記制御手段は、前記第 1 の通信装置と前記第 2 の通信装置との間の通信履歴を前記記憶手段に書き込む。

【 0 0 1 4 】

また、第 1 の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる前記第 2 の通信装置の処理結果を、前記要求の送信元の前記第 1 の通信装置に送信する。

【 0 0 1 5 】

また、第 1 の発明の通信制御装置は、好ましくは、前記制御手段は、前記受信手段から受信した情報に応じて、待機状態にある前記第 1 の通信装置が動作状態になるように制御する。

【 0 0 1 6 】

また、第 1 の発明の通信制御装置は、好ましくは、前記制御手段は、前記第 1 の通信装置が接続されたネットワークと、前記第 2 の通信装置が接続されたネッ

トワークとの間の通信を制御する。

【 0 0 1 7 】

また、第 1 の発明の通信制御装置は、好ましくは、前記装置識別情報は、前記第 1 の通信装置の製造元で付された当該通信装置を一意に識別可能な識別子である。

【 0 0 1 8 】

また、第 1 の発明の通信制御装置は、好ましくは、前記利用者識別情報は、登録した利用者に予め割り当てられた識別子である

請求項 1 に記載の通信制御装置。

【 0 0 1 9 】

また、第 2 の発明の通信システムは、単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信システムであって、前記通信制御装置は、前記第 1 の通信装置を識別するための装置識別情報を記憶する第 1 の記憶手段と、前記第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報と利用者識別情報とを含む要求を前記第 2 の通信装置に送信する第 1 の送信手段と、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する第 1 の受信手段と、前記応答に含まれる前記装置識別情報と前記第 1 の記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記第 1 の記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する制御手段とを有し、前記第 2 の通信装置は、前記要求を受信する第 2 の受信手段と、前記利用者識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する第 2 の記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記利用者識別情報に対応する前記送信先の情報を前記第 2 の記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果と前記要求に含まれる前記装置識別情報とを対応付けて送信する第 2 の送信手段とを有する。

【 0 0 2 0 】

また、第 3 の発明の通信方法は、単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信方法であって、前記第 1 の通信装置から前記通信制御装置に出された要求に応じて、当該第 1 の通信装置に対応する装置識別情報と利用者識別情報とを含む要求を前記通信制御装置から前記第 2 の通信装置に送信し、前記第 2 の通信装置において、受信した前記要求に応じた所定の処理を行い、前記第 2 の通信装置において、前記要求に含まれる前記利用者識別情報に対応する送信先の情報に基づいて、前記処理の結果と前記要求に含まれる前記装置識別情報とを含む応答を前記通信制御装置に送信し、前記通信制御装置において、受信した前記応答に含まれる前記装置識別情報と、予め保持した前記第 1 の通信装置の前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、正当な前記第 1 の通信装置によるものであるかを判断する。

## 【 0 0 2 1 】

## 【発明の実施の形態】

以下、本発明の実施形態に係わるトランザクション認証システムについて説明する。

図 1 は、本実施形態のトランザクション認証システム 1 0 1 の全体構成図である。

図 1 に示すように、トランザクション認証システム 1 0 1 では、例えば、発注者 3 1 の発注者端末装置 1 1 と、受注者 3 3 の受注者端末装置 1 5 と、ネットワーク銀行 4 0 の認証装置 5 0 とが、インターネットなどの外部ネットワーク（通信網） 9 を介して接続されており、発注者 3 1 と受注者 3 3 との間のトランザクション（取引）の正当性を認証装置 5 0 で認証する。

なお、当該ネットワークに接続されているホームネットワークシステム（発注者端末システム） 1 0 および受注者端末装置 1 5 の数は任意である。

## 【 0 0 2 2 】

本実施形態では、ホームネットワークシステム 1 0 が本発明の通信制御装置に対応し、端末装置 1 1<sub>1</sub> ～ 1 1<sub>4</sub> が本発明の第 1 の通信装置に対応し、認証装置 5 0 が本発明の第 2 の通信装置に対応している。

## 【 0 0 2 3 】

本実施形態では、例えば、発注者 3 1 および受注者 3 3 とネットワーク銀行 4 0 との間で認証を行うことについての契約が成されている。また、発注者 3 1 と引き落とし銀行 4 2 との間では、例えば、ネットワーク銀行 4 0 によって認証された取引引きに関する引き落としを行う旨の契約がなされている。また、ネットワーク銀行 4 0 と保険会社 4 3 との間では、ネットワーク銀行 4 0 が係わった電子商取引によって生じた損害についての保険契約がなされている。

## 【 0 0 2 4 】

以下、トランザクション認証システム 1 0 1 を構成する各装置について説明する。

## 〔ホームネットワークシステム 1 0〕

図 1 および図 2 に示すように、ホームネットワークシステム 1 0 は、発注者 3 1 の各家庭などに構築されており、ホームネットワークシステム 1 0 のホームゲートウェイ 1 2 が、図 1 に示す受注者端末装置 1 5 および認証装置 5 0 が接続される外部ネットワーク 9 に有線あるいは無線で接続されている。

また、ホームゲートウェイ 1 2 には、例えば、家庭内の内部ネットワーク 1 3 を介して、端末装置 1 1<sub>1</sub> , 1 1<sub>2</sub> , 1 1<sub>3</sub> , 1 1<sub>4</sub> が有線あるいは無線で接続される。

端末装置 1 1<sub>1</sub> ~ 1 1<sub>4</sub> は、例えば、デジタルテレビ受信装置、パーソナルコンピュータ、電話機およびゲーム機などである。

端末装置 1 1<sub>1</sub> ~ 1 1<sub>4</sub> の各々には、例えば製造元で当該端末装置を識別するための装置 ID 情報が割り当てられており、当該装置 ID 情報が各端末装置の内部メモリに記憶されている。例えば、端末装置 1 1<sub>1</sub> には装置 ID 情報 ID<sub>M1</sub> が割り当てられ、端末装置 1 1<sub>2</sub> には装置 ID 情報 ID<sub>M2</sub> が割り当てられ、端末装置 1 1<sub>3</sub> には装置 ID 情報 ID<sub>M3</sub> が割り当てられ、端末装置 1 1<sub>4</sub> には装置 ID 情報 ID<sub>M4</sub> が割り当てられている。

## 【 0 0 2 5 】

図 3 は、ホームゲートウェイ 1 2 の構成図である。

ホームゲートウェイ 1 2 は、例えば、外部ネットワーク I / F 6 1、内部ネッ

トワーク I / F 6 2、暗号化部 6 3、復号部 6 4、記憶部 6 5、制御部 6 6 および署名検証部 6 7 を有する。

ここで、外部ネットワーク I / F 6 1 および内部ネットワーク I / F 6 2 が、第 1 の発明の送信手段および受信手段、並びに第 2 の発明の第 1 の送信手段および第 2 の受信手段に対応している。また、記憶部 6 5 が、第 1 の発明の記憶手段および第 2 の発明の第 1 の記憶手段に対応している。また、制御部 6 6 が第 1 の発明および第 2 の発明の制御手段に対応している。

#### 【 0 0 2 6 】

外部ネットワーク I / F 6 1 は、外部ネットワーク 9 を介して認証装置 5 0 との間で、情報あるいは要求の送受信を行なう。

内部ネットワーク I / F 6 2 は、内部ネットワーク 1 3 を介して端末装置 1 1<sub>1</sub> ~ 1 1<sub>4</sub> との間で、情報あるいは要求の送受信を行なう。

暗号化部 6 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 6 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 6 5 は、例えば、ホームゲートウェイ 1 2 の電源が投入されたときに電源がオンになっている端末装置 1 1<sub>1</sub> ~ 1 1<sub>4</sub> から内部ネットワーク 1 3 を介して受信した装置 ID 情報 ID<sub>M1</sub> ~ ID<sub>M4</sub> を記憶している。

また、記憶部 6 5 は、発注者 3 1 が作成した秘密鍵 K<sub>31,S</sub>などを格納する。

署名検証部 6 7 は、例えば、認証装置 5 0 が作成した署名情報を、ネットワーク銀行 4 0 の公開鍵 K<sub>40,P</sub>を用いて検証する。

制御部 6 6 は、発注者端末装置 1 1 内の各構成要素の処理を統括的に制御する。

制御部 6 6 は、ホームゲートウェイ 1 2 を介した端末装置 1 1<sub>1</sub> ~ 1 1<sub>4</sub> と認証装置 5 0 との間の通信の履歴を示す履歴情報を生成し、これを記憶部 6 5 に記憶する。

そのため、記憶部 6 5 に記憶された履歴情報にアクセスを行うだけで、家庭内に設けられた端末装置 1 1<sub>1</sub> ~ 1 1<sub>4</sub> を用いた通信の履歴を簡単に知ることができ、管理が容易になる。

#### 【 0 0 2 7 】

また、制御部 6 6 は、例えば、待機状態（スタンバイ状態）になっている端末装置 1 1<sub>1</sub> ~ 1 1<sub>4</sub> に対してのアクセスを、外部ネットワーク 9 を介して受けた場合に、対応する端末装置 1 1<sub>1</sub> ~ 1 1<sub>4</sub> が動作状態になるように制御する。

## 【 0 0 2 8 】

制御部 6 6 は、例えば、発注者 3 1 による操作に応じて端末装置 1 1<sub>1</sub> ~ 1 1<sub>4</sub> から内部ネットワーク I / F 6 2 が受信した、発注情報 a 1 と、個人キー情報 k 1 と（本発明の利用者識別情報）、個人 ID 情報 ID 1（本発明の利用者識別情報）と、装置 ID 情報 ID<sub>M1</sub> ~ ID<sub>M4</sub>（本発明の装置識別情報）との全体に対して暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求 Inf 1 を生成する。

また、制御部 6 6 は、例えば、認証要求 Inf 1 を認証装置 5 0 に送信した後、認証装置 5 0 から認証応答 Inf 4 を受信したときに、認証応答 Inf 4 に含まれる認証要求の送信元の装置を示す装置 ID 情報と、記憶部 6 5 から読み出した装置 ID 情報 ID<sub>M1</sub> ~ ID<sub>M4</sub> の何れかが一致するか否かを検出し、一致している場合には、正当な取り引きが行われていると判断し、不一致の場合には、不正な取り引きが行われたと判断して、その旨を受注者端末装置 1 5 および認証装置 5 0 の少なくとも一方に通知する。

## 【 0 0 2 9 】

## 〔受注者端末装置 1 5〕

図 4 に示すように、受注者端末装置 1 5 は、サイバーモール (Cyber Mall) などに店舗を出している受注者 3 3 が使用するサーバ装置であり、受信部 7 1、送信部 7 2、暗号化部 7 3、復号部 7 4、記憶部 7 5、制御部 7 6 および署名検証部 7 7 を有する。

受信部 7 1 は、外部ネットワーク 9 を介して認証装置 5 0 から情報あるいは要求を受信する。

送信部 7 2 は、外部ネットワーク 9 を介して認証装置 5 0 に情報あるいは要求を送信する。

また、受信部 7 1 および送信部 7 2 は、発注者端末装置 1 1 からのアクセスに応じて、例えば、記憶部 7 5 から読み出した受注者 3 3 が提供する商品等の案内



情報を、ネットワークを介して、発注者端末装置 1 1 に送信する。

暗号化部 7 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 7 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 7 5 は、受注者 3 3 が作成した秘密鍵  $K_{33,S}$  などを格納する。

制御部 7 6 は、受注者端末装置 1 5 内の各構成要素の処理を統括的に制御する。

署名検証部 7 7 は、例えば、ネットワーク銀行 4 0 の公開鍵  $K_{40,P}$  を用いて、認証装置 5 0 が作成した署名情報の検証を行う。

【 0 0 3 0 】

〔認証装置 5 0〕

図 5 に示すように、認証装置 5 0 は、受信部 8 1、送信部 8 2、暗号化部 8 3、復号部 8 4、記憶部 8 5、制御部 8 6、署名作成部 8 7 および課金処理部 8 8 を有する。

【 0 0 3 1 】

ここで、受信部 8 1 が第 2 の発明の第 2 の受信手段に対応し、送信部 8 2 が第 2 の発明の第 2 の送信手段に対応し、記憶部 8 5 が第 2 の発明の第 2 の記憶手段に対応し、制御部 8 6 が第 2 の発明の処理手段に対応している。

【 0 0 3 2 】

受信部 8 1 は、外部ネットワーク 9 を介してホームゲートウェイ 1 2 および受注者端末装置 1 5 から情報あるいは要求を受信する。

送信部 8 2 は、外部ネットワーク 9 を介してホームゲートウェイ 1 2 および受注者端末装置 1 5 に情報あるいは要求を送信する。

暗号化部 8 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 8 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 8 5 は、発注者 3 1 がネットワーク銀行 4 0 と契約したときに、発注者 3 1 の個人キー情報  $k_1$  と、個人 ID 情報  $ID_1$  と、ホームゲートウェイ 1 2 のアドレスとの対応表を記憶する。また、記憶部 8 5 は、例えば、発注者 3 1 および受注者 3 3 がネットワーク銀行 4 0 と契約をしたときに、発注者 3 1 が作成した秘密鍵  $K_{31,S}$  に対応する公開鍵  $K_{31,P}$ 、並びに受注者 3 3 が作成した秘密鍵  $K$

33,Sに対応する公開鍵 $K_{33,P}$ などを格納する。

制御部 8 6 は、認証装置 5 0 内の各構成要素の処理を統括的に制御する。

署名作成部 8 7 は、ネットワーク銀行 4 0 の秘密鍵 $K_{40,S}$ を用いて署名情報の作成を行う。

課金処理部 8 8 は、発注者 3 1 による取り引きに関する認証に対しての課金処理を行う。

認証装置 5 0 の各構成要素の詳細な処理については、後述する動作例で記載する。

### 【 0 0 3 3 】

以下、トランザクション認証システム 1 0 1 の動作例を説明する。

当該動作例では、図 2 に示す発注者 3 1 が図 2 に示す端末装置 1 1<sub>1</sub> を操作して、受注者 3 3 が提供する商品またはサービスの発注を行なう場合を説明する。

なお、当該動作例を開始する前提として、以下の手続および処理が行なわれている。

すなわち、発注者 3 1 とネットワーク銀行 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 4 0 は、発注者 3 1 に対して、個人キー情報  $k_1$  および個人 ID 情報 ID 1 を発行する。

ネットワーク銀行 4 0 は、個人キー情報  $k_1$  と、個人 ID 情報 ID 1 と、ホームゲートウェイ 1 2 のアドレスとの対応表を図 5 に示す認証装置 5 0 の記憶部 8 5 に記憶する。ここで、個人キー情報  $k_1$  は、例えば、ネットワーク銀行 4 0 と契約した契約者（発注者 3 1）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報 ID 1 は、発注者 3 1 の銀行口座番号などの課金に係わる情報を示す識別子である。

### 【 0 0 3 4 】

また、ネットワーク銀行 4 0 は、自らの秘密鍵 $K_{40,S}$ を図 5 に示す認証装置 5 0 の記憶部 8 5 に記憶すると共に、当該秘密鍵 $K_{40,S}$ に対応する公開鍵 $K_{40,P}$ をホームゲートウェイ 1 2 および受注者端末装置 1 5 に送信する。ホームゲートウェイ 1 2 は、公開鍵 $K_{40,P}$ を図 3 に示す記憶部 6 5 に記憶する。受注者端末装置 1 5 は、公開鍵 $K_{40,P}$ を図 4 に示す記憶部 7 5 に記憶する。

## 【 0 0 3 5 】

また、受注者 3 3 とネットワーク銀行 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 4 0 は、受注者 3 3 に対して、個人キー情報 Z および個人 ID 情報 ID 2 を発行する。ネットワーク銀行 4 0 は、個人キー情報 Z および個人 ID 情報 ID 2 の対応表を図 5 に示す認証装置 5 0 の記憶部 8 5 に記憶する。

## 【 0 0 3 6 】

また、ホームゲートウェイ 1 2 の電源が投入されたときに電源がオンになっている端末装置 1 1<sub>1</sub> ~ 1 1<sub>4</sub> から内部ネットワーク 1 3 を介してホームゲートウェイ 1 2 が受信した装置 ID 情報 ID<sub>M1</sub> ~ ID<sub>M4</sub> が、図 3 に示す記憶部 6 5 に記憶される。

## 【 0 0 3 7 】

図 6 は、トランザクション認証システム 1 0 1 の動作例を説明するための図である。

## ステップ S T 1 1 :

図 1 に示す発注者 3 1 は、例えばネットワーク上の商店である受注者 3 3 に商品を発注する場合に、発注する商品名および数量などを示す発注情報 a 1 と、発注者 3 1 の個人キー情報 k 1 と、発注者 3 1 の個人 ID 情報 ID 1 とを、図示しない操作手段を操作して端末装置 1 1<sub>1</sub> に入力する。なお、発注情報 a 1 には、受注者 3 3 を特定する情報が含まれている。

端末装置 1 1<sub>1</sub> は、当該入力された発注情報 a 1 と、発注者 3 1 の個人キー情報 k 1 と、発注者 3 1 の個人 ID 情報 ID 1 と、内部メモリから読み出した装置 ID 情報 ID<sub>M1</sub> とを、内部ネットワーク 1 3 を介して、ホームゲートウェイ 1 2 に送信する。

## 【 0 0 3 8 】

## ステップ S T 1 2 :

図 3 に示すホームゲートウェイ 1 2 は、発注情報 a 1 と、個人キー情報 k 1 と、個人 ID 情報 ID 1 と、装置 ID 情報 ID<sub>M1</sub> とを内部ネットワーク I / F 6 2 で受信し、これらの全体に対して暗号化部 6 3 で暗号化を行う。

ホームゲートウェイ 1 2 は、当該暗号化した情報を格納した認証要求 Inf 1

(本発明の要求)を、図3に示す外部ネットワークI/F61から外部ネットワーク9を介して、図1に示すネットワーク銀行40の認証装置50に送信する。

#### 【0039】

##### ステップST13:

図5に示す認証装置50は、ホームゲートウェイ12からの認証要求Inf1を受信部81が受信すると、記憶部85からネットワーク銀行40の秘密鍵 $K_{40,S}$ を読み出し、復号部84において、当該秘密鍵 $K_{40,S}$ を用いて認証要求Inf1を復号する。

次に、認証装置50は、制御部86の制御に基づいて、上記復号した認証要求Inf1に格納された発注情報a1および個人キー情報k1を格納した情報Inf1' について、記憶部85から読み出した自らの秘密鍵 $K_{40,S}$ を用いて署名情報Au1を作成する。

次に、認証装置50は、情報Inf1' および署名情報Au1を格納した要求Inf2を生成する。

次に、暗号化部83は、図5に示す記憶部85から読み出した受注者33の公開鍵 $K_{33,P}$ を用いて、上記生成した要求Inf2を暗号化した後に、送信部82から、外部ネットワーク9を介して受注者端末装置15に送信する。

#### 【0040】

##### ステップST14:

受注者端末装置15の復号部74は、認証装置50からの要求Inf2を受信部71が受信すると、記憶部75から読み出した自らの秘密鍵 $K_{33,S}$ を用いて、要求Inf2を復号する。

次に、受注者端末装置15の署名検証部77は、上記復号した要求Inf2に格納された署名情報Au1を、記憶部75から読み出した認証装置50の公開鍵 $K_{40,P}$ を用いて検証する。

#### 【0041】

受注者端末装置15の制御部76は、署名検証部が上記検証の結果、署名情報Au1の正当性が認証されると、要求Inf2に格納された情報Inf1' を図4に示す記憶部75に記憶する。受注者33は、情報Inf1' 内の発注情報a

1に基づいて、発注者31への商品等の発送予定などを示す受注確認情報c1を生成する。

次に、制御部76は、要求Inf2、受注確認情報c1および自らの個人キー情報Zを格納した応答Inf3を生成する。

次に、受注者端末装置15の送信部72は、上記生成した応答Inf3を、記憶部75から読み出したネットワーク銀行40の公開鍵 $K_{40,P}$ を用いて暗号化部73で暗号化した後に、送信部72から、外部ネットワーク9を介して認証装置50に送信する。

受注者33は、例えば、要求Inf2に格納された情報Inf1'内の発注情報a1に基づいて、発注者31が発注した商品等を発注者31に発送したり、発注者31が注文したサービスを発注者31に提供する。

【0042】

ステップST15：

認証装置50の復号部84は、受注者端末装置15からの応答Inf3を受信部81が受信すると、記憶部85から読み出した自らの秘密鍵 $K_{40,S}$ を用いて、Inf3を復号し、要求Inf1に格納された発注情報a1と、当該復号されたInf3に格納された受注者33の個人キー情報Zとを用いて、所定の取り引き履歴情報を作成し、これを記憶部85に格納する。当該履歴情報は、ネットワーク銀行40が、発注者31に対して決済を行う際に用いられる。

また、認証装置50の署名作成部87は、ステップST14で受信した応答Inf3について、自らの秘密鍵 $K_{40,S}$ を用いて署名情報Au2を作成する。

次に、認証装置50の制御部86は、応答Inf3および署名情報Au2を格納した認証応答Inf4を作成する。

次に、認証装置50の暗号化部83は、上記作成した認証応答Inf4を、記憶部85から読み出した発注者31の公開鍵 $K_{31,P}$ を用いて暗号化する。

そして、図5に示す記憶部85に個人ID情報ID1と対応して記憶されているホームゲートウェイ12のアドレスを用いて、送信部82から外部ネットワーク9を介してホームゲートウェイ12に当該暗号化した応答Inf4を送信する。

ホームゲートウェイ 1 2 では、受信した認証応答  $I n f 4$  を、図 3 示す記憶部 6 5 から読み出した発注者 3 1 の秘密鍵  $K_{31,S}$  を用いて復号部 6 4 で復号する。

次に、ホームゲートウェイ 1 2 の署名検証部 6 6 は、当該復号した認証応答  $I n f 4$  に格納された署名情報  $A u 2$  を、記憶部 6 5 から読み出したネットワーク銀行 4 0 の公開鍵  $K_{40,P}$  を用いて検証すると共に、 $I n f 4$  内の発注情報  $a 1$  内に記述された装置 ID 情報  $I D_{M1}$  が図 3 に示す記憶部 6 5 に記憶されている装置 ID 情報  $I D_{M1} \sim I D_{M4}$  の何れかと一致するか否かを判断する。当該動作例では、一致すると判断され、発注者 3 1 と受注者 3 3 との間の当該取り引きが正当に行われたことが確認される。

#### 【 0 0 4 3 】

##### ステップ S T 1 6 :

ホームゲートウェイ 1 2 は、応答  $I n f 4$  に含まれる  $I n f 3$  を、内部ネットワーク 1 3 を介して端末装置 1 1<sub>1</sub> に送信する。

端末装置 1 1<sub>1</sub> は、当該受信した  $I n f 3$  に格納された受注確認情報  $c 1$  をディスプレイなどに表示する。

#### 【 0 0 4 4 】

以下、発注者 3 1 の個人 ID 1 および個人キー  $k 1$  を不正に取得した図 1 に示す不正者 5 5 が自らの端末装置である不正者端末装置 5 6 を用いて、認証装置 5 0 に認証要求を送信した場合のトランザクション認証システム 1 0 1 の動作を説明する。

図 7 は、トランザクション認証システム 1 0 1 の当該動作を説明するための図である。

##### ステップ S T 2 1 :

図 1 に示す不正者 5 5 は、受注者 3 3 に商品を発注する場合に、発注する商品名および数量などを示す発注情報  $a 1$  と、不正に取得した発注者 3 1 の個人キー情報  $k 1$  と、不正に取得した発注者 3 1 の個人 ID 情報  $I D 1$  とを、図示しない操作手段を操作して不正者端末装置 5 6 に入力する。

不正者端末装置 5 6 は、発注情報  $a 1$  と、個人キー情報  $k 1$  と、個人 ID 情報  $I D 1$  と、内部メモリから読み出した装置 ID 情報  $I D_{M56}$  を暗号化し、当該暗

号化した情報を格納した認証要求  $I n f 1$  を、外部ネットワーク 9 を介して、図 1 に示すネットワーク銀行 4 0 の認証装置 5 0 に送信する。

図 5 に示す認証装置 5 0 は、不正者端末装置 5 6 からの認証要求  $I n f 1$  を受信部 8 1 が受信すると、当該認証要求  $I n f 1$  について、前述したステップ  $S T 1 2$  と同様の処理を行なう。

【 0 0 4 5 】

ステップ  $S T 2 2$  :

ステップ  $S T 2 2$  の処理は、前述したステップ  $S T 1 3$  の処理と同じである。

【 0 0 4 6 】

ステップ  $S T 2 3$  :

ステップ  $S T 2 3$  の処理は、前述したステップ  $S T 1 4$  の処理と同じである。

【 0 0 4 7 】

ステップ  $S T 2 4$  :

ステップ  $S T 2 4$  の処理は、前述したステップ  $S T 1 5$  の処理と同じである。

【 0 0 4 8 】

ステップ  $S T 2 5$  :

ステップ  $S T 2 5$  の処理は、前述したステップ  $S T 1 6$  の処理と同じである。

【 0 0 4 9 】

このように、トランザクション認証システム 1 0 1 によれば、不正者 5 5 が不正者端末装置 5 6 を用いて、認証要求  $I n f 1$  を認証装置 5 0 に送信した場合でも、その応答である認証応答  $I n f 4$  は、認証装置 5 0 の記憶部 8 5 に個人 ID 情報  $I D 1$  と対応して記憶されているホームゲートウェイ 1 2 のアドレスに基づいて、ホームゲートウェイ 1 2 に送信される。

これにより、ホームゲートウェイ 1 2 において、認証応答  $I n f 4$  に含まれる装置 ID 情報  $I D_{M56}$  が、図 3 に示す記憶部 6 5 に記憶されている装置 ID 情報  $I D_{M1} \sim I D_{M4}$  と一致しないと判断され、発注者 3 1 の個人 ID 情報  $I D 1$  を用いた不正な認証要求が行なわれたことを検出できる。

そのため、トランザクション認証システム 1 0 1 によれば、他人の個人 ID 情報を用いた不正な取り引きを効果的に抑制できる。

## 【 0 0 5 0 】

上述したように、トランザクション認証システム 1 0 1 によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などを費用を低額にでき、電子商取引をさらに普及させることが可能になる。

## 【 0 0 5 1 】

また、トランザクション認証システム 1 0 1 によれば、例えば、図 1 および図 2 に示す端末装置 1 1<sub>1</sub> からの要求に応じて認証要求 I n f 1 を認証装置 5 0 に送信した後に、端末装置 1 1<sub>1</sub> が故障した場合でも、当該認証要求 I n f 1 に応じた認証応答 I n f 4 に応じた処理を適切に行うことができる。

## 【 0 0 5 2 】

また、トランザクション認証システム 1 0 1 によれば、外部ネットワーク 9 を介した通信に伴うセキュリティに関する機能をホームゲートウェイ 1 2 に持たせることで、端末装置 1 1<sub>1</sub> ～ 1 1<sub>4</sub> に備えるセキュリティ機能のレベルを下げることができ、端末装置 1 1<sub>1</sub> ～ 1 1<sub>4</sub> の構成を簡単かつ安価にできる。

## 【 0 0 5 3 】

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、本発明の第 2 の通信装置として認証処理を行う認証装置 5 0 を例示したが、第 2 の通信装置が行う処理はその他、課金処理などであってもよい。

また、上述した実施形態では、ネットワーク銀行 4 0 が、認証装置 5 0 を用いて、トランザクション（取り引き）の認証業務を行う場合を例示したが、ネットワーク銀行 4 0 とは別の機関が、認証装置 5 0 を用いてトランザクションの認証業務を行うようにしてもよい。

## 【 0 0 5 4 】

また、上述した実施形態では、端末装置 1 1<sub>1</sub> ～ 1 1<sub>4</sub> の装置 I D 情報を認証装置 5 0 に送信した場合を例示したが、ホームゲートウェイ 1 2 の装置 I D 情報を認証装置 5 0 に送信するようにしてもよい。

## 【 0 0 5 5 】



## 【発明の効果】

以上説明したように、本発明によれば、不正に取得した他人の識別情報（個人 I D 情報）に基づいて不正な認証手続きが行われることを回避する通信制御装置、通信システムおよびその方法を提供できる。

また、本発明によれば、複数の通信装置を用いてネットワークを介した電子商取引などを行う場合に、当該電子商取引に必要な機能の割り当て、並びに通信履歴の管理を効率的に行うことができる通信制御装置、通信システムおよびその方法を提供できる。

## 【図面の簡単な説明】

## 【図 1】

図 1 は、本発明の実施形態のトランザクション認証システムの全体構成図である。

## 【図 2】

図 2 は、図 1 に示すホームネットワークシステムを説明するための図である。

## 【図 3】

図 3 は、図 2 に示すホームゲートウェイの構成図である。

## 【図 4】

図 4 は、図 1 に示す受注者端末装置の構成図である。

## 【図 5】

図 5 は、図 1 に示す認証装置の構成図である。

## 【図 6】

図 6 は、正当者が認証要求を出した場合の図 1 に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

## 【図 7】

図 7 は、不正者が認証要求を出した場合の図 1 に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

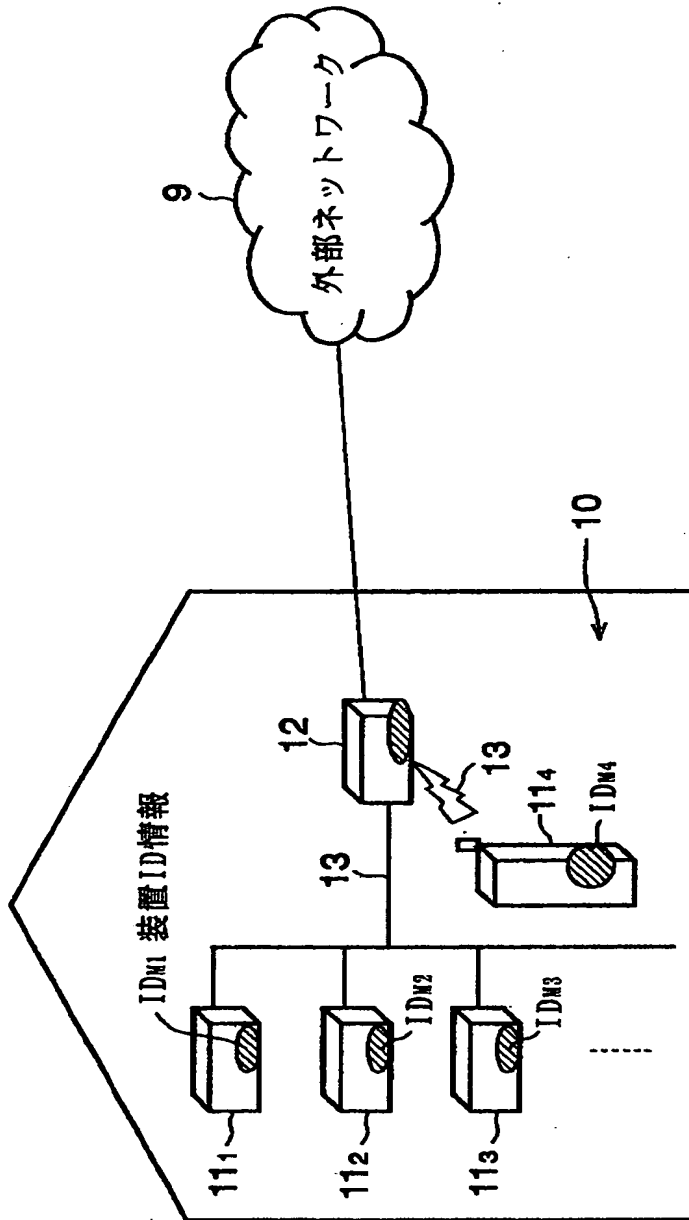
## 【符号の説明】

1 … トランザクション認証システム、11 … 発注者端末装置、15 … 受注者端末装置、31 … 発注者、33 … 受注者、40 … ネットワーク銀行、50 … 認証装

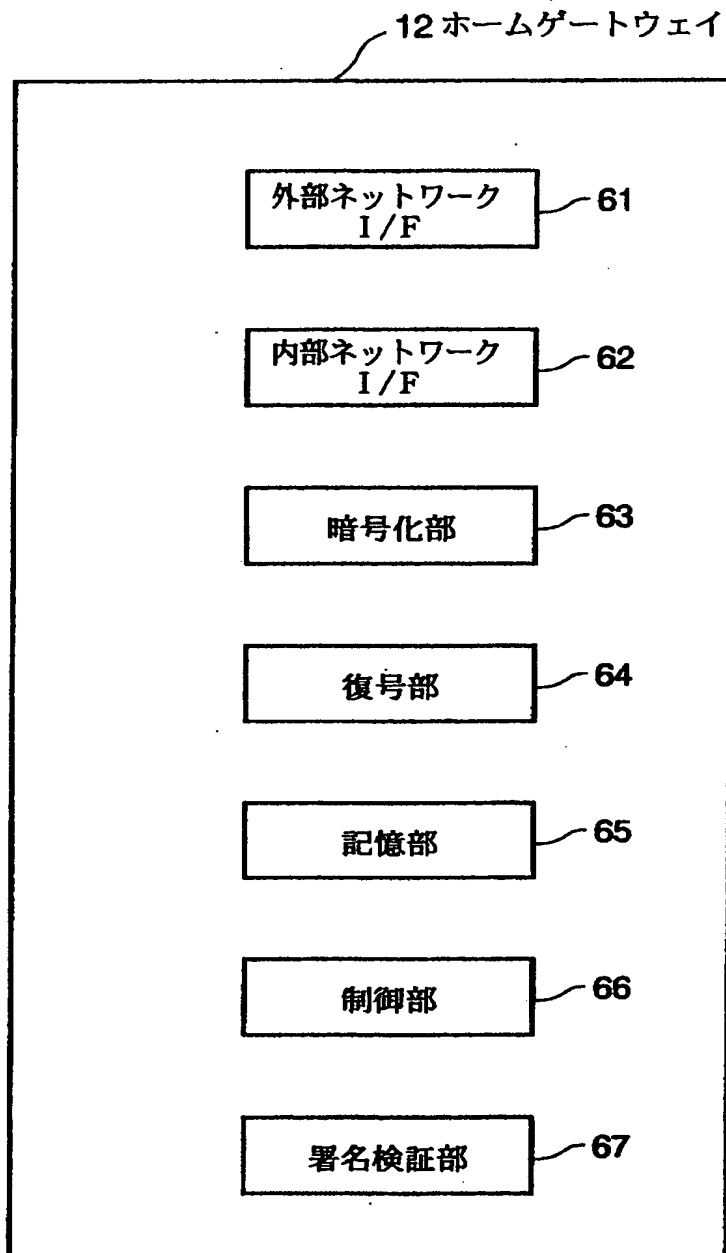
置、6 1…外部ネットワーク I/F、6 2…内部ネットワーク I/F、7 1, 8  
 1…受信部、7 2, 8 2…送信部、6 3, 7 3, 8 3…暗号化部、6 4, 7 4,  
 8 4…復号部、6 5, 7 5, 8 5…記憶部、6 6, 7 6, 8 6…制御部、6 7,  
 7 7…署名検証部、, 8 7…署名作成部、8 8…課金処理部、a 1…発注情報、  
 k 1…発注者 3 1 の個人キー情報 k 1、I D 1…発注者 3 1 の個人 I D 情報、I  
 D<sub>M1</sub>, I D<sub>M2</sub>, I D<sub>M3</sub>, I D<sub>M4</sub>, I D<sub>M56</sub>…装置 I D 情報、A u 1, A u 2…認  
 証装置の署名情報、Z…受注者の個人キー情報、I n f 1…認証要求、I n f 4  
 …認証応答



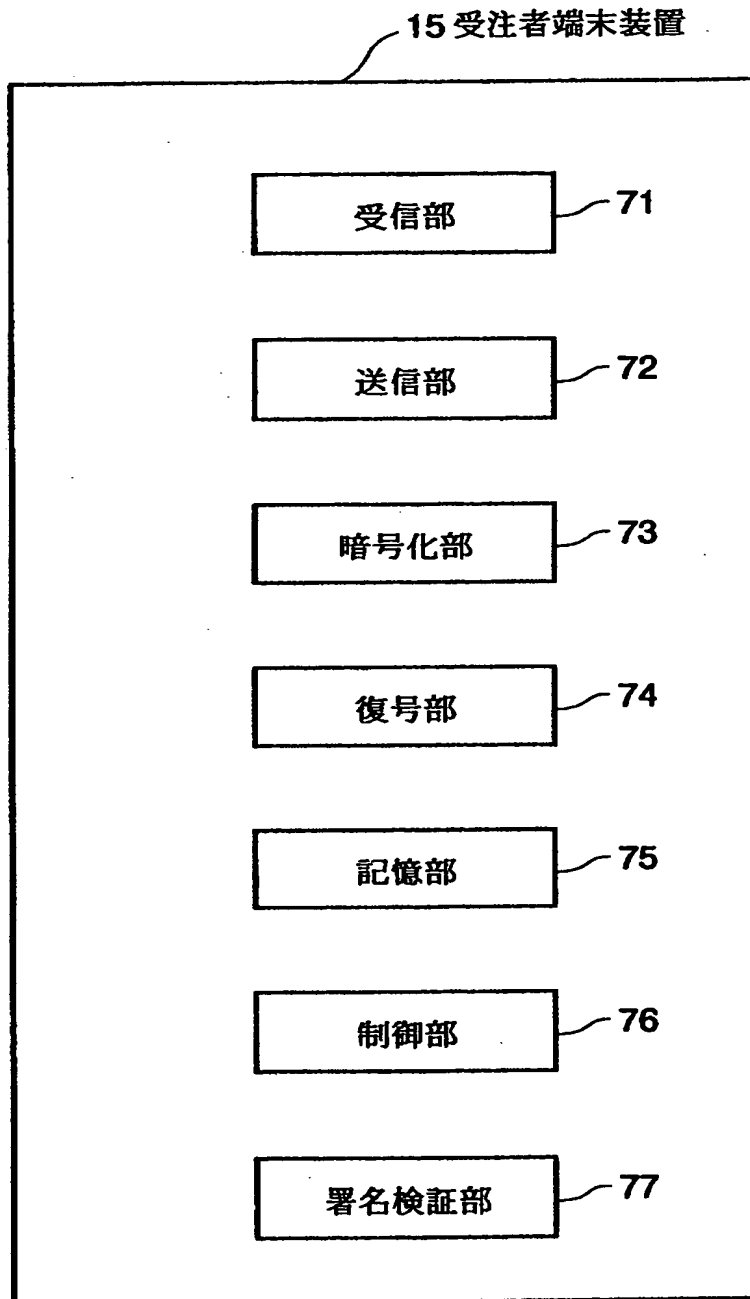
【図2】



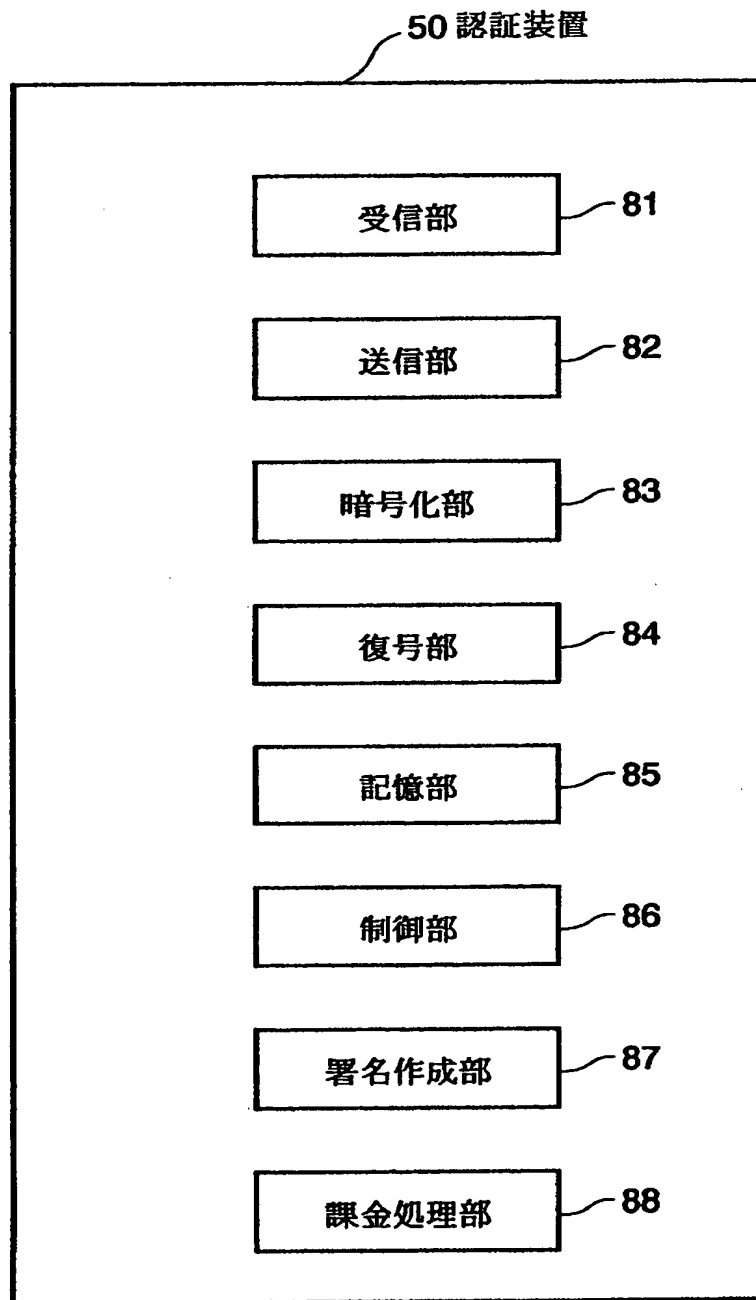
【図 3】



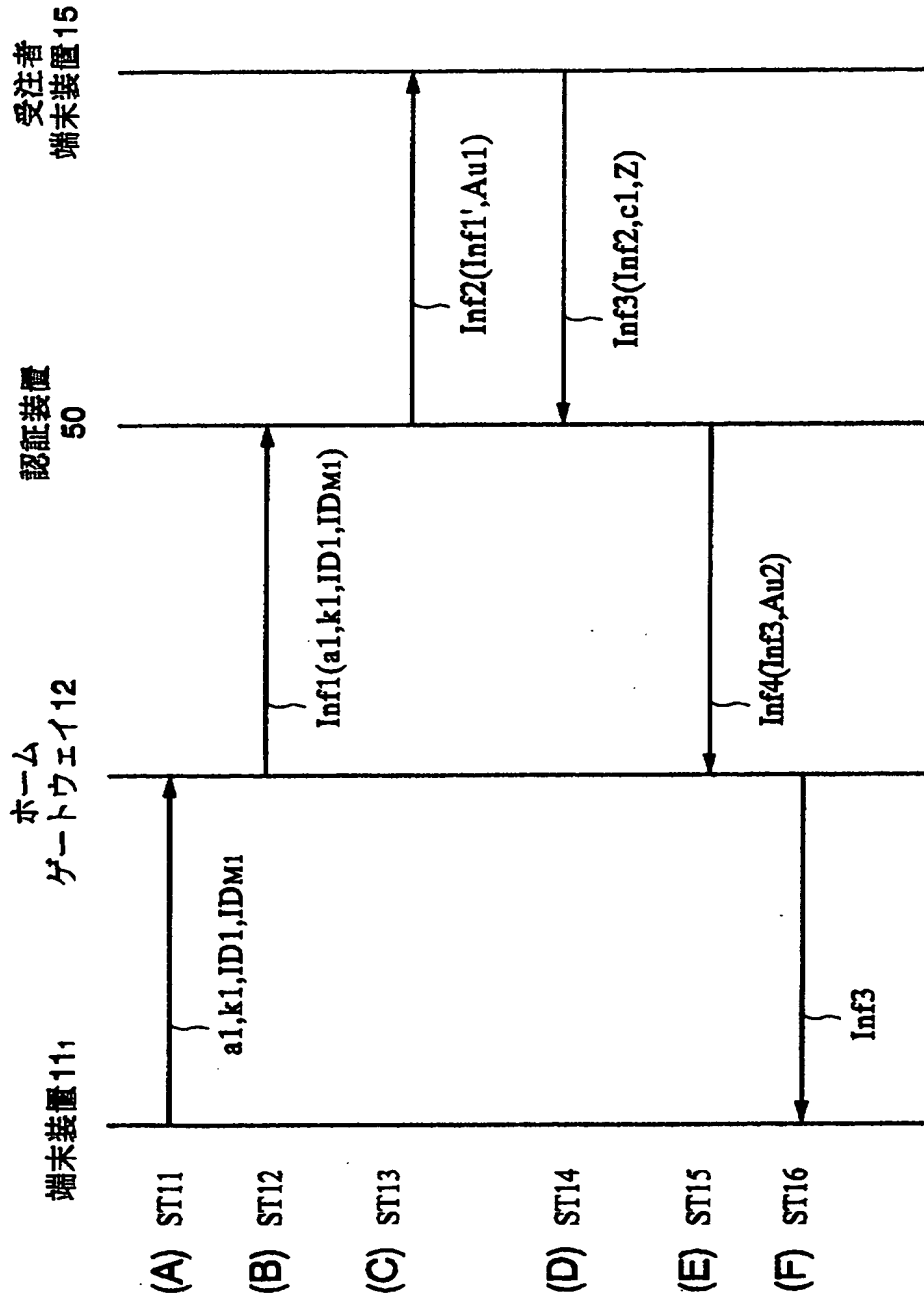
【図4】



【図 5】

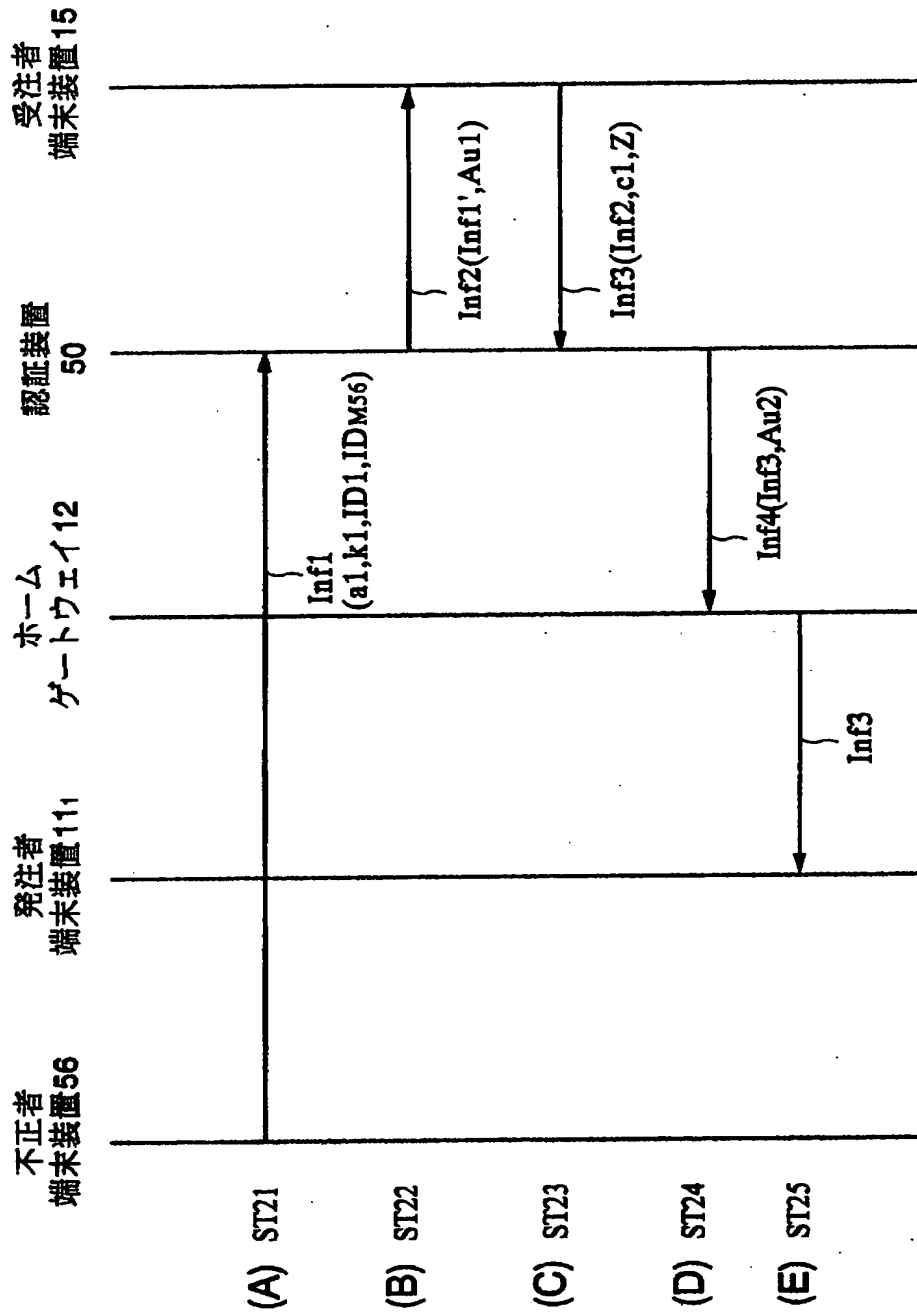


【図 6】





【図 7】



【書類名】 要約書

【要約】

【課題】 不正に取得した他人の個人 I D 情報に基づいて不正な手続が行われることを回避する通信制御装置を提供する。

【解決手段】 ホームゲートウェイ 1 2 は、端末装置 1 1<sub>1</sub> ~ 1 1<sub>4</sub> を識別するための装置識別情報 I D<sub>M1</sub> ~ I D<sub>M4</sub> を記憶し、端末装置 1 1 からの要求に応じて、当該端末装置に対応する装置識別情報を含む要求を認証装置 5 0 に送信し、前記要求の送信元の装置を識別するための装置識別情報を含む応答を認証装置 5 0 から受信し、当該応答に含まれる装置識別情報と、前記記憶している装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、正当な端末装置 1 1 によるものであるかを判断する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 2 1 8 5]

1. 変更年月日	1 9 9 0 年 8 月 3 0 日
[変更理由]	新規登録
住 所	東京都品川区北品川 6 丁目 7 番 3 5 号
氏 名	ソニー株式会社

This Page Blank (uspto)